savvius™

WHITE PAPER

The Definitive Guide to 802.11ac Packet Capture

The IEEE 802.11ac standard is changing the rules when it comes WLAN troubleshooting based on packet capture and analysis. Packet-based analysis is unquestionably the most complete and most accurate approach for WLAN troubleshooting, but 802.11ac is challenging the software, equipment, and processes required to perform packet-based analysis. This white paper explains how 802.11ac is changing the rules for 802.11ac packet capture, and what you can do about it.

Contents

Introduction

802.11ac, which was officially ratified by the IEEE in December 2013, is now the de facto WLAN standard. According to IDC, as of 2015, 802.11ac accounted for almost 50% of access point (AP) shipments and nearly 63% of AP revenues. In 2016, the standard is expected to make up the majority of revenue and shipments. This represents a noticeably faster adoption rate than the 802.11n transition several years ago. This is great news for the WLAN industry as well as enterprises interested in improving the performance and range of their WLANs.

But 802.11ac is a game-changer not just in the area of performance. It also will bring about changes in network design, implementation, management, and troubleshooting.

This paper addresses the impacts of 802.11ac on traditional packet-based WLAN analysis and troubleshooting. WLAN industry veterans know that packet-based analysis is the most complete and most accurate approach when it comes to WLAN troubleshooting. The equipment, software, and processes required to perform packet-based analysis for 802.11ac requires rethinking, and possibly retooling. Let's examine exactly how 802.11ac is changing the rules for 802.11ac packet capture, and what you can do about it.

802.11ac – Impact on WLAN Analysis

The key changes in 802.11ac that affect packet-based WLAN analysis are increased speed and capacity (number of users per AP with good quality), and wide-spread variations in the capabilities of equipment.

Increased Speed and Capacity

802.11ac is approximately three times faster (based on peak data rates) than 802.11n, given similar hardware. This may not seem revolutionary at first, but when you consider a 3-stream device, that's the difference between 450Mbps for 802.11n and 1.3Gbps for 802.11ac. With .11ac, we're breaking the gigabit barrier! And with more users able to connect reliably to a single AP, the result is substantially more data, and in the lingo of packet-based analysis, far more packets being processed per AP, which means far more packets that need to be analyzed by your packet-based network analysis software.

Variations in Equipment Capabilities

As 802.11 specifications have evolved, especially the core specifications like a/b/g/n/ac, more and more configuration options have been introduced. From a product perspective, this means that client devices (stations) and APs don't always have the same capabilities, and in general, APs and other infrastructure hardware (repeaters, for example) have greater capabilities than stations.

At first glance this may not seem like a problem at all, and it's typically not a problem from a WLAN design and operation perspective. However, it's a game-changer for WLAN analysis. Packet-based WLAN analysis has traditionally been done in a "portable" fashion – a laptop running packet-based network analysis software is carried into the area where troubleshooting is required, and a commercial WLAN adapter, typically in a USB form factor, is used as the capture device to feed packets to the analyzer. For 802.11a/b/g this worked very well, since every device, station and AP alike, was capable of sending data at all the supported data rates. So any WLAN adapter could be used to capture all of the data on a WLAN. With 802.11n, and even more so with 802.11ac, APs have more capability than even the most capable USB WLAN adapters, which limits the effectiveness of these adapters in performing WLAN analysis.

[1] http://www.networkworld.com/article/2226675/wi-fi/what-s-next-for-enterprise-wireless-lans-.html

Four Limitations Today

Network Data Capture at the Point of Failure

First, given the pervasive deployments of WLANs, it is becoming less likely that a network engineer can always be in the vicinity of a problem that requires troubleshooting. WLAN troubleshooting requires that data be captured within a few hundred feet of the source of the problem. There is no way around this; it's a matter of physics. As WLANs become more widespread, network engineers must adopt solutions that enable them to capture data remotely for WLAN troubleshooting and analysis.

Network Analysis at Gigabit Speeds

The availability of high performance network analysis solutions is another critical issue. With Wave 1 of 802.11ac, AP data rates achieved up to 1.3Gbps. This means that the analysis software for WLANs must have the same performance capability as that of gigabit Ethernet LANs. Most WLAN analysis software was originally designed to handle only one-tenth the data rates of 802.11ac, or less, including popular open source solutions like Wireshark, and other commercially available software. Care must be exercised to ensure that the analysis software can handle the 802.11ac data rates, especially with the introduction of Wave 2 and even higher aggregate data rates.

USB is Not up to the Task

In addition to network analysis platforms, USB bus speeds and WLAN USB adapters are simply not up to the task of 802.11ac packet capture. Many laptops in use for WLAN analysis still have USB v2.0 ports. USB 2.0 has a maximum theoretical speed of 480 Mbps, and a practical limit of 280 Mbps. This is clearly falls far short of the rates possible with 802.11ac Wave 2. Even "Super Speed" USB v3.0, with its effective throughput of 3.2 Gbps, will barely make the grade for future 802.11ac performance scenarios. This means that even if both the 802.11ac USB adapter and the laptop support USB 3.0, there are still 802.11ac scenarios that cannot be fully analyzed using this traditional technique.

Capture Support for 3- or 4-Stream 11ac Data

Perhaps the most significant USB limitation is that even the most capable adapters support only 2-stream 802.11ac. This translates to a maximum throughput of 867Mbps. Devices with this throughput limitation will capture only 1- and 2-stream 802.11ac data. Any 3- or 4-stream data on the WLAN will simply be ignored. Because the USB adapter is unable to capture these packets, the network cannot be effectively monitored or analyzed for troubleshooting. Clearly, this not acceptable for an analysis solution that you trust for reporting on everything about your WLAN environment.

It is unlikely that 3- and 4-stream USB WLAN adapters will ever come to market. The primary use case for a USB WLAN adapter is to add 802.11 networking support to a device that currently does not have it. As technology advances, 802.11 networking is being built into every device imaginable, eliminating the need for USB WLAN adapters.

802.11ac – Changing the Rules

Given the new capabilities of 802.11ac, and the limitations with current methodologies for performing WLAN analysis and troubleshooting, a shift in thinking is required. Let's review all the methodologies available for detailed WLAN analysis, both the "tried and true" as well as new approaches, and see how they stack up for 802.11ac WLAN analysis.

Portable Monitoring and Analysis

Portable analysis has been the approach of choice for WLAN network analysts for years. Portable analysis requires that the analyst be in the vicinity of the wireless problem – within a few hundred feet. It uses a laptop with WLAN analysis software, and supported WLAN adapters that can be placed in promiscuous, or “sniffing” mode, which are then used to capture wireless packets for the software to analyze. Supported WLAN adapters are either integrated into the laptop (typically mini PCIe cards inside the laptop), or, more commonly, are external USB WLAN adapters.

USB adapters have become more popular since analysts typically want to capture from multiple channels simultaneously, requiring an adapter for each channel. USB technology readily supports multiple connected devices making this an excellent choice. The whole configuration is portable since it is all contained within, and powered by, a single laptop. Analysts can easily move about, finding the best location to capture data. Portable analysis is often used by wireless consultants and field engineers for WLAN equipment manufacturers, for whom portability is a key requirement.

There are two significant drawbacks to portable analysis. First, you need to be where the problem is, which is getting more and more difficult (and expensive) as enterprise WLANs become more widespread. And second, the USB WLAN adapters typically used for packet capture are not keeping pace with 802.11ac technology. Most adapters are 1-stream 11ac, with a few 2-stream choices that support packet capture, while enterprise 11ac APs are at 3-stream and 4-stream (Wave 2). A 1-stream WLAN USB adapter will only see 1-stream 11ac (or 11n) data. Any packets from equipment using 2 or more streams will simply be ignored. The adapter and the software won’t even know of the existence of these packets. So users of portable analysis with 11ac (or 11n) must be very clear on what they hope to achieve when performing analysis.

Remote Monitoring and Analysis

The main difference between portable and remote analysis is that remote analysis employs devices that are already in the area where analysis is required, and uses those devices to capture wireless packets and send them back over the wired network to the wireless analysis software. This enables the wireless analyst to remain “remote”, while still analyzing the same wireless data that they would have captured if they had travelled to the site and done portable analysis.

There are three primary approaches that can be used to capture wireless packets for remote analysis–dedicated WLAN sensors, dedicated appliances with WLAN adapters, and APs.

Savvius’s Omnipeek network analyzer supports both dedicated appliances and APs for remote packet capture. If dedicated appliances are used, this is a special case of remote analysis called distributed analysis, which we cover in the next section.

Using an 802.11ac AP as a remote packet capture device has significant advantages:

- The APs are already part of the network and inherently have the capacity to capture whatever traffic is on your WLAN.
- APs are located exactly where you need them to capture 802.11 packets, eliminating the need for additional sensors or “overlay” networks for monitoring.
- When designed with appropriate overlap, one or several APs in a WLAN can be used as packet capture devices, or in promiscuous mode, without disrupting WLAN operation. When not in capture mode, the AP simply increases the overall coverage and performance of the WLAN.

Remote analysis using APs to capture data does pose a few challenges. Most APs must be controller-based to operate in packet capture, or "sniffer" mode, although some standalone APs can also operate in this mode (none for 802.11ac so far). Once put into this mode, most APs lose the capability to continue acting as network devices, meaning any users who had been associated with the AP will migrate to adjacent APs, hence the need for sufficient AP overlap for this technique to be most effective.

Our recommendation is to simply plan ahead for the use of APs for WLAN analysis, and budget for certain AP to always act as sensors, providing you with always-available data for WLAN analysis when you need it. Since APs in packet capture mode are quite sensitive, and don't need to be concerned with being close enough to clients to guarantee a given data rate, you need far fewer APs for packet capturing than you do for WLAN data delivery.

Distributed Monitoring and Analysis

Distributed WLAN analysis uses the deployed APs in exactly the same way as in remote analysis, but it allows the packet analysis to be performed locally to the AP controller, eliminating the transmission of all the wireless packets across the wired network to the remote network analyzer software. This is the preferred approach when the wireless data volume is large. It also provides the capability for ongoing, 24x7 analysis with the ability to store all captured packets locally.

With the dispersed nature of most WLAN deployments today, the mission-critical data that is transmitted, and the significantly increased volume of data that 802.11ac will drive 24x7 WLAN analysis is really the only viable option.

Distributed WLAN analysis requires the placement of the analysis software at the same location as the WLAN controller. This software can be hosted on your own appliance, or on a purpose-built appliance supplied by Savvius. All WLAN traffic that is being captured for analysis terminates at this device, and the device analyzes the data and stores packets per the configuration options set by the user.

Distributed monitoring and analysis gives you the best of both worlds. It allows the analyst to remain remote, while providing ongoing, 24x7 analysis of the WLAN. Reported issues can be addressed quickly, and the analytical results are always just a click away.

Wireless Forensics

Distributed monitoring and analysis leads to a unique capability – wireless forensics. The distributed approach allows you to record all WLAN data to the analysis appliance. Wireless issues can then be analyzed both in real-time or post-incident (wireless forensics). This is especially useful since most WLAN trouble tickets are filed after an event occurs. Analysis can now be done on the event, as it happened, with no need to try to duplicate the problem, or wait for it to happen again. For mission-critical wireless applications, for example, real-time financial applications, 24x7 analysis and recording also allows analysts to verify if specific application transactions are properly executed, providing unequivocal proof when transactions are questioned, or for compliance reporting.

Configuring APs for Remote Packet Capture

Using APs for remote packet capture is a critical capability as new methodologies for WLAN analysis are employed. Configuring APs for packet capture is quite simple. There are two different methods, depending on the capabilities of the AP. These methods are described briefly below. For more detailed configuration information, please see our guide “Configuring APs for Remote Packet Capture”.

Remote Pcap

Remote Pcap is a standard method supported by many enterprise AP manufacturers, including Aerohive, Ruckus, and Xirrus. Using the Remote Pcap interface, the user directs the network analyzer to connect to an AP that supports Remote Pcap (via the Remote Pcap daemon). Once the connection is established, the AP sends a list of supported Remote Pcap interfaces back to the analyzer. The user then chooses which interfaces to use and manually starts the capture.

The main advantage with using Remote Pcap is that it is a de-facto standard - no custom software is required, and all supported devices will operate in a consistent manner. However, the challenge is in discovering which APs support Remote Pcap. The best way to do this is to contact the manufacturer directly.

Custom Remote Adapters

Custom remote adapters provide a connection to APs that do not support Remote Pcap. Custom remote adapters are specific to the Omnipeek network analyzer software, and provide a proprietary tunnel to APs from supported vendors. These APs must first be put into packet capture, or “sniffer” mode, via the UI for the controller to which the AP is connected. The controller UI is also used to set the channel on which packets will be captured, and what bandwidth will be used. Multiple APs can be configured to capture packets and send the data to Omnipeek. Omnipeek has custom remote adapters for Aruba and Cisco.

Access Point Capture and Wi-Fi Analysis - Rules for the Road

Using APs for packet capture does not require a separate overlay network for monitoring, significantly reducing the overall capital expenditure for WLAN monitoring and analysis. When done correctly, it provides the most cost-effective and flexible remote WLAN analysis system. Here are some WLAN design factors that should be considered for AP-based remote packet capture:

- **Additional AP coverage**
  When using APs as packet capture devices, the wireless network must have sufficient AP overlap. Typically, overlapping coverage is already a part of any well-designed WLAN deployment. This allows WLAN clients to maintain adequate data rates and performance, even when roaming. Since remote AP packet capture could take certain APs offline while in sniffer mode, additional overlap should be factored into the design to compensate for one or more APs being unavailable for client access.

- **Dedicated APs for packet capture**
  It's a good idea to designate certain APs as sniffer-only devices so that they are dedicated to data capture 24x7. This simplifies the AP coverage design since this approach will eliminate the need to take APs offline. This is especially important for wireless forensics, which is used to continuously capture, store, and analyze data. Forensics is well suited for high-throughput networks, or WLAN analysis systems that are capturing packets from a large number of APs simultaneously. It provides a complete recording of all WLAN traffic, so any and all problems are captured and recorded as they happen. This eliminates the time consuming task of reproducing complex, intermittent problems that are common with wireless networks. Network forensics also provides a complete history of WLAN activity for transaction verification in mission-critical deployments, such as financial applications.

- **Not every problem on the WLAN is a wireless problem**
  Wired analysis must be part of the total monitoring and troubleshooting solution. Problems are just as likely to occur on the wired side of the connection, especially for authentication issues when using WPA-2 Enterprise, or for application-layer issues. Using a single solution that can perform both wired and wireless analysis enables seamless comparison of traffic from both sides of the AP, and reduces the learning curve for network analysts.

- **Portable analysis isn't dead - but know the limitations**
  Using a portable device for WLAN analysis and troubleshooting is definitely still a viable option, but users need to be very aware of the limitations. Capturing 802.11ac data with USB WLAN adapters will not always provide adequate results. Most USB WLAN adapters are limited to 2-stream 802.11ac operation (867 Mbps), so any traffic that exceeds this data rate will simply be invisible to an analysis session. This approach is still feasible in cases where the analysis is limited just to clients that operate under 867 Mbps. However if the problem being investigated is not well characterized, you will need to see all of the WLAN traffic, and a USB based solution will not meet your needs.

- **WLAN analysis software must be powerful**
  Don't forget that the demands on WLAN analysis software are also much greater with 802.11ac. Many WLAN analysis systems were originally designed to handle 802.11b/g data rates – nothing in excess of 54 Mbps. Processing packets in real time at 1.3 Gbps or greater is beyond their capabilities. Be sure that your WLAN network analysis software meets the demands of multi-gigabit real-time packet processing. Systems that are designed for both wired and wireless analysis are much more likely to be capable of meeting these demands.

Savvius Solutions for 802.11ac

Savvius WLAN Analysis Solution Advantages

The Savvius Omnipeek solution is the first to support data capture and analysis of 802.11ac traffic delivering significant system value:

- Exclusive support for:
  - ◊ Data capture via inexpensive, commercially available devices
  - ◊ Remote data capture that leverages the current network of deployed enterprise APs
  - ◊ Comprehensive voice-over-wireless (VoFi) analysis
  - ◊ Multi-channel and wireless roaming analysis
- Optimal support for distributed networks with remote 24x7 real-time analysis
- Effortless and comprehensive troubleshooting with an industry-leading user interface
- Both wireless and wired network analysis in the single solution
- Investment protection you can count on with Savvius' history of early support for new 802.11 standards and vendor hardware

Conclusion

Wireless LANs have become pervasive and mission critical in enterprise organizations, large and small. The sheer performance and capacity of 802.11ac will continue this trend as it approaches Ethernet speeds. This, in combination with the exponential growth of smart phones, hybrids, and tablets accelerates the need for network reliability and uptime. In addition, 802.11ac introduces new challenges in WLAN analysis and troubleshooting. Network analysis solutions, such as Savvius Omnipeek, cost effectively address these challenges, while continuing to protect your network investments.

About Savvius

Savvius, Inc. brings 25 years as a leader in network performance and security forensics solutions to customers in more than 60 countries worldwide. Savvius's Omnipliance®, OmniPeek®, and Savvius Vigil™ products enable network and security professionals to identify, understand, and respond to network performance issues and the need for post-breach insight. Savvius customers include Apple, Boeing, Cisco, Fidelity, Microsoft, and over half of the Fortune 100. For more information, please visit www.savvius.com.

For more information, please visit www.savvius.com or call +1 (925) 937-3200.

More Resources

You'll find white papers and other resources here:

https://www.savvius.com/learn